CLINICAL CONSULTATION INFORMATION SHARING METHOD

Patent Number: JP10111897
Publication date: 1998-04-28
Inventor(s): KIDO KUNIHIKO; SANO KOICHI
Applicant(s): HITACHI LTD
Requested Patent: ☐ JP10111897
Application Number: JP19960265745 19961007
Priority Number(s):
IPC Classification: G06F19/00; G06F17/60; G06F17/30; G09C1/00
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To share clinical consultation data on condition that the privacy of an individual is protected and security is secured by providing a means which adds an access control setting file as one attribute of medical consultation information of a patient of each medical organ, and exchanging clinical consultation information on the patient according to the access control setting file.
SOLUTION: A hospital 101 and a hospital 102 performs a mutual authenticating process about whether or not they have the right to exchange clinical consultation data on the patient A. Then a random number R generated on the side of the hospital 101 is sent together with the ID number of the patient A according to the address HOSP of a file server 105 of the hospital 102 in the access control setting file. The file server 105 of the hospital 102 takes the mutual authentication key Ak of the access control setting file out of a clinical consultation data storage file of the patient A. Then Ak(R) generated by ciphering the random number R with the authentication key Ak and the random number R generated at the hospital 102 are sent back to the hospital 101 according to the address HOSP of a file server 104 of the hospital 101 in the access control setting file.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－111897

(43)公開日　平成10年(1998)４月28日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	19/00		Ｇ０６Ｆ	15/42	Ｈ
	17/60		Ｇ０９Ｃ	1/00	６６０Ｄ
	17/30		Ｇ０６Ｆ	15/21	３６０
Ｇ０９Ｃ	1/00	６６０		15/40	３２０Ｂ
				15/42	Ｊ

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願平8－265745

(22)出願日　平成８年(1996)10月７日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　木戸　邦彦
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　佐野　耕一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　診療情報共有化方法

(57)【要約】
【課題】複数医療機関にまたがり患者の診療データを共有する際に、患者のプライバシー保護と安全性を確保した上で、診療データ共有化を図ることを目的とする。
【解決手段】患者ごとに、複数の医療機関のネットワーク１０３上でのアドレス一覧が記述されたテーブルと、当該患者のために割り当てた暗号化用の鍵と、各医療機関同士の相互認証処理に使用する鍵を含むファイルを患者当人が任意に作成する手段と、前記ファイルが確かに当該患者に関するものであることを各医療機関が認証する手段と、前記ファイルを各医療機関の当該患者の診療情報の一属性として付加する手段を有し、前記ファイルに基づき形成される各医療機関間での当該患者のための安全なアクセス経路を介して、当該患者の診療情報を安全に共有化する。

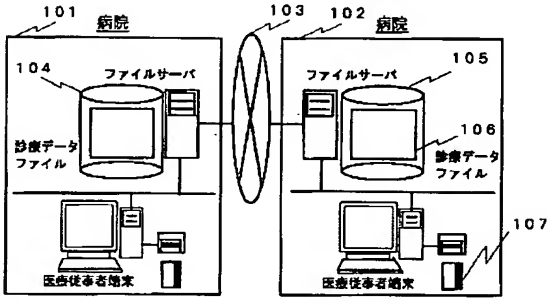


図1

【特許請求の範囲】
【請求項１】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報システムにおいて、患者ごとに、複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルと、当該患者のために割り当てた暗号化用の鍵と、各医療機関同士の相互認証処理に使用する鍵を含むアクセス制御設定ファイルを作成する手段と、前記アクセス制御設定ファイルが確かに当該患者に関するものであることを各医療機関が認証する手段と、前記アクセス制御設定ファイルを各医療機関の当該患者の診療情報の一属性として付加する手段を有し、前記アクセス制御設定ファイルに基づき当該患者の診療情報を安全に交換することを特徴とする診療情報共有化方法。
【請求項２】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報システムにおいて、複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルと、当該患者のために割り当てた暗号化用の鍵と、各医療機関同士の相互認証処理に使用する鍵を含むアクセス制御設定ファイルを、可搬媒体が有する記憶装置に記憶して管理することを特徴とする請求項１の診療情報共有化方法。
【請求項３】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報システムにおいて、請求項１のアクセス制御設定ファイルに含まれる複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルについて、新たに追加される医療機関は、前記テーブルに含まれるネットワーク上の各アドレスに対して、当該医療機関のアドレスを送付することを特徴とする請求項１の診療情報共有化方法。
【請求項４】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報システムにおいて、患者に対する診療データの通信に際しては、請求項１のアクセス制御設定ファイルに含まれる相互認証処理に使用する鍵で相互認証し、暗号化用の鍵で暗号化して通信することを特徴とする請求項１の診療情報共有化方法。
【請求項５】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報システムにおいて、患者は、請求項１のアクセス制御設定ファイルに患者固有の秘密鍵で電子署名したものを、前記アクセス制御設定ファイルに含まれる複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルの各アドレスに送信することを特徴とする請求項１の診療情報共有化方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数医療機関において、患者の診療情報を安全に共有する手段を提供するものであり、広域医療情報システムに関する。
【０００２】
【従来の技術】複数医療機関をまたいで、診療情報を共有する方法として、患者のプライバシー保護の観点から、保健医療カードとよばれるＩＣカードで行われ場合が多い。ＩＣカードは、患者本人が携帯しており、本人がそのカードを第３者に貸したり、譲渡しない限り、カードの中身の安全性が保たれる。加えて、ＩＣカードには、カード自体にマイクロプロセッサが埋め込まれていて、そのマイクロプロセッサで暗証番号によるアクセス権のチェックが行える。従って、ＩＣカード内のデータは、ＩＣカードにアクセス権限のない不特定な第３者に知られることはない。通常、このアクセス権限は、カード所有者本人や医師などに与えられるのが普通である。
【０００３】
【発明が解決しようとする課題】このように、ＩＣカードに情報を記録して、複数医療機関で診療情報を共有する方法は、強固なプライバシー保護が達成できる反面、医師の手元にカードがない限り患者情報を調べることができない不便さがある。例えば、ある患者が複数の医療機関を同時に受診している場合、各医療機関で処方された薬品、最近行われた検査結果、診断内容等をその患者を受け持っている各主治医が把握することは大切であるが、患者がカードを携帯して主治医のもとに来た時以外、カード内の情報を得ることができない。従って、主治医が、患者の来院前にその患者の各種情報を前もって調べておき、今後の診断治療に役立てるなどの行為は事実上不可能である。このように、ＩＣカードをベースとして、複数医療機関で診療情報を共有する方法では、患者に対する情報を主治医が知りたいときにタイムリーに得ることができないという問題がある。
【０００４】
【課題を解決するための手段】患者ごとに、複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルと、当該患者のために割り当てた暗号化用の鍵と、各医療機関同士の相互認証処理に使用する鍵を含むファイルを患者当人が任意に作成する手段と、前記ファイルが確かに当該患者に関するものであることを各医療機関が認証する手段と、前記ファイルを各医療機関の当該患者の診療情報の一属性として付加する手段を有し、

前記ファイルに基づき形成される各医療機関間での当該患者のための安全なアクセス経路を介して、当該患者の診療情報を安全に共有化することにより達成することができる。

【０００５】

【発明の実施の形態】

「実施例１」本発明の実施の形態として、ある患者Ａが２つの医療機関を受診した場合について説明する。まず、実施例１として、上記、患者Ａ専用の安全なアクセス経路を形成するためのアクセス制御設定ファイル２０１を共有する手段として、ＩＣカードを利用する場合について説明する。図１は、システム全体の構成について説明したものである。また、図２は、本実施例で使用するファイルの構成を示したものである。この図では、病院１０１と病院１０２の二つのエンティティ間での患者Ａの診療データ共有を想定している。ここで、患者Ａは、病院１０２を受診した後に、病院１０１を受診したとする。病院１０１と病院１０２は、病院外部のネットワーク１０３に公開されたファイルサーバ１０４、１０５を持つ。ファイルサーバ１０４、１０５には、病院で診察治療を受けた患者のカルテデータが登録されている。この図では、ファイルサーバ１０５にある患者Ａの診療データ１０６が登録されていると想定している。患者Ａは保健医療カード１０７を所持している。ここで、保健医療カードとは、診察カード、保険カードなど、保健医療に関るＩＣカードなどのセキュアな媒体を意味する。

【０００６】「アクセス制御設定ファイル生成と診療データファイル生成」保健医療カード１０７内のアクセス制御設定ファイル生成と患者Ａの診療データファイル生成について説明する。

【０００７】（１）患者Ａは、アクセス制御設定ファイル２０１の生成を保健医療カード１０７に指示する。この時、保健医療カード１０７の鍵生成モジュール３０２において、乱数Ｒ１を生成し、これをカード内のマスタ鍵により暗号化して鍵Ｄｋを生成し、アクセス制御設定ファイル記憶領域３０１の暗号化用鍵の記憶領域３０３に登録する。同様に、保健医療カード１０７の鍵生成モジュール３０２は、乱数Ｒ２を生成し、これをカード内のマスタ鍵により暗号化して鍵Ａｋを生成し、アクセス制御設定ファイル記憶領域３０１の相互認証用鍵の記憶領域３０４に登録する。（図３）

（２）病院１０２は、ファイルサーバ１０５に患者Ａ用の診療データファイルを作成する。そして、病院１０２を訪れた患者Ａは、アクセス制御設定ファイル記憶領域３０１の医療機関のアドレステーブル３０５に病院１０２のアドレスＨＯＳＰ２を登録してもらう。

【０００８】（３）（２）の処理を、患者Ａは病院１０１に訪れたときにも行う。病院１０１は、ファイルサーバ１０４に患者Ａ用の診療データファイルを作成する。そして、アクセス制御設定ファイル記憶領域３０１の医療機関のアドレステーブル１１２に病院１０１のアドレスＨＯＳＰ１を登録してもらう。

【０００９】ここで、上記、病院１０１および１０２のアドレスとは、ファイルサーバ１０４と１０５のネットワーク１０３の所在のことである。

【００１０】「アクセス制御設定情報の設定」保健医療カード１０７内のアクセス制御設定ファイルに基づき、患者Ａの診療データファイルにアクセス制御設定情報をセットする手続きについて説明する。

【００１１】（１）病院１０１においては、患者Ａが来院したときに、アクセス制御設定ファイル２０１の内容を、保健医療カード１０７のアクセス制御設定ファイル記憶領域３０１から読みとれば良い。これにより、病院１０１は、アクセス制御設定ファイル２０１の暗号化用鍵、相互認証鍵、そして病院１０２のアドレスＨＯＳＰ２を得ることが可能である。

【００１２】（２）病院１０２においても同様に、アクセス制御設定ファイル２０１の内容を、保健医療カード１０７のアクセス制御設定ファイル記憶領域３０１から読みとる。ここで、病院１０２では、アクセス制御設定ファイル２０１の暗号化用鍵、相互認証鍵に関する情報は、保健医療カード１０７から読み取ることが可能であるが、アドレステーブル２０５は空欄である。従って、病院１０２を受診した患者Ａが、その後に受診した病院について（この実施例では病院１０１）のアドレスは、別手段で得る必要がある。ここでは、病院１０１から次の手段で病院１０１のアドレスを配送してもらう。病院１０１は、（１）で読みとったアクセス制御設定ファイル２０１の医療機関のアドレステーブル１１２をサーチする。この例の場合には、病院１０２のみが登録されているので、そのアドレスのみを取り出す。そして、アクセス制御設定ファイル２０１の相互認証用鍵で病院１０２と病院１０１の相互認証を行った後に、患者ＡのＩＤ番号とともに病院１０１のアドレスＨＯＳＰ１をアクセス制御設定ファイル２０１の暗号化用鍵で暗号化して病院１０２に送る。以上により、病院１０２は、患者Ａに対する、アクセス制御設定ファイル２０１の暗号化用鍵、相互認証鍵、そして病院１０１のアドレスＨＯＳＰ１を得ることができた。ここで、上記、アクセス制御設定ファイル２０１の医療機関のアドレステーブル１１２をサーチした時点で、複数医療機関のアドレスが登録されている場合には、その病院すべてに自分のアドレス（この場合、病院１０１のアドレス）をマルチキャストする。

【００１３】（３）（１）（２）により、病院１０１および病院１０２において得られたアクセス制御設定情報は、病院１０１および病院１０２において、ファイルサーバ１０４、１０５における患者Ａの診療データファイル２０６（電子カルテデータ）のアクセス制御設定情報

２０８に取り込み診療情報の一属性として管理する。

【００１４】診療データの場合、患者のプライバシー保護の観点から、安全なアクセス経路を規定する情報（上記実施例のファイル２０１）は、当該患者の診療データの一属性として管理する必要がある。また、アクセス制御設定ファイル２０１が、確かに患者Ａのものであるという認証は、患者Ａが各病院を訪れた際に、信頼できる第３者機関により発行された保健医療カードを患者から直に受けとり、アクセス制御設定ファイル２０１の情報を得ていることにより保証される。

【００１５】次に、患者Ａの診療情報を、病院１０１と病院１０２がネットワーク１０３を介して通信しあいデータ交換を図る手段について説明する。例えば、病院１０１が病院１０２の患者Ａの診療データファイル１０６を参照するとする。次に、図４の説明をする。

【００１６】（１）病院１０１と病院１０２は、患者Ａの診療データ交換を行う権利があるかどうか相互認証処理を行う。ここでは、相互認証処理として３パス相手認証方法を適用する。

【００１７】１）患者ＡのＩＤ番号とともに、病院１０１側で生成した乱数Ｒを、アクセス制御設定ファイル２０１の病院１０２のファイルサーバ１０５のアドレスＨＯＳＰ２に基づき送信する。

【００１８】２）病院１０２のファイルサーバ１０５は、患者Ａの診療データ保存ファイルから、アクセス制御設定ファイル２０１の相互認証鍵Ａｋを取り出す。そして、Ａｋで乱数Ｒを暗号化したＡｋ（Ｒ）と病院１０２で生成した乱数Ｓを、アクセス制御設定ファイル２０１の病院１０１のファイルサーバ１０４のアドレスＨＯＳＰ１に基づき病院１０１に送り返す。

【００１９】以降、病院１０１と病院１０２の通信は、アドレスＨＯＳＰ１、ＨＯＳＰ２に基づき行うものとする。

【００２０】３）病院１０１は、送られてきたＡｋ（Ｒ）を、相互認証鍵Ａｋで復号し、１）で送信した乱数Ｒと一致すれば、病院１０１は病院１０２が患者Ａの診療データを所有していることがわかる。もし一致しなければ、以降の処理を中止し、患者Ａの診療データ交換を中止する。

【００２１】４）病院１０１は、乱数Ｓを相互認証用鍵Ａｋで暗号化したＡｋ（Ｓ）を病院１０２に送信する。

【００２２】５）病院１０２は、送られてきたＡｋ（Ｓ）を相互認証用鍵Ａｋで復号し、２）で送信した乱数Ｓと比較する。一致すれば、病院１０２は、病院１０１が患者Ａの診療データへのアクセス権を有することが分かる。もし一致しなければ、以降の処理を中止し、患者Ａの診療データ交換を中止する。

【００２３】（２）病院１０２のファイルサーバ１０５は、本セッションにおけるデータ暗号化用セッション鍵とデータ認証用セッション鍵を生成する。

【００２４】１）患者Ａの診療データ保存ファイルから、アクセス制御設定ファイル２０１の暗号化処理用鍵Ｄｋを取り出す。

【００２５】２）病院１０２のファイルサーバ１０５は、乱数Ｔ１，Ｔ２を生成し、暗号化処理用鍵Ｄｋにより暗号化して、データ暗号化用セッション鍵ＤＴｋとデータ認証用セッション鍵ＭＴｋを生成する。

【００２６】（３）（２）で生成した、データ暗号化用セッション鍵ＤＴｋとデータ認証用セッション鍵ＭＴｋを、病院１０２は相互認証用鍵Ａｋで暗号化したＡｋ（ＤＴｋ）とＡｋ（ＭＴｋ）を病院１０１に送信する。病院１０１は、（３）で送られてきたＡｋ（ＤＴｋ）とＡｋ（ＭＴｋ）を復号して、データ暗号化用セッション鍵ＤＴｋとデータ認証用セッション鍵ＭＴｋを取り出す。

【００２７】（４）病院１０２は、診療データ１０６に対して、所定のハッシュ関数によりメッセージダイジェストを生成し、データ認証用セッション鍵ＭＴｋで暗号化した認証コードを作成する。次に、生成した認証コードを診療データ１０６に付加したものを、データ暗号化用セッション鍵ＤＴｋで暗号化する。これを、病院１０１に送信する。

【００２８】（５）病院１０１では、（４）で送られてきたデータについて、データ暗号化用セッション鍵ＤＴｋで復号し、診療データ１０６と認証コードを取り出し、診療データ１０６に対して、所定のハッシュ関数によりメッセージダイジェストを生成し、データ認証用セッション鍵ＭＴｋで暗号化した認証コードを送られた認証コードと比較する。一致すれば正しい患者Ａの診療データである。

【００２９】以上により、病院１０１と病院１０２の間で、データ認証とデータ暗号化により、患者Ａに関する診療データを安全に共有化することが可能となる。ここで、上記構成をとることによる一つの特徴がある。病院１０１は、来院した患者Ａの情報は病院１０２のファイルサーバから参照することは可能であるが、病院１０１に来院していない患者の診療データは参照不可能である。これは、患者Ａの診療データ交換を行う権利があるかどうか、患者Ａの相互認証用鍵で相互認証処理を行い、この処理で相互認証が成立しない限りデータ交換が行えないからである。この特徴により、患者の主治医あるいは主治医が在籍する病院以外からの診療データ参照が不可能になるため、患者のプライバシー保護が可能になる。

【００３０】本発明のもう一つの特徴について説明する。まず最初に、診療データについての特徴について簡単に説明する。診療データは、ある患者の診療の過程で発生したデータを蓄積したものであるから、それを記録する主治医とともに患者自身の所有物と考えられる。すなわち、診療データには、利用者（医療従事者）とその

所有者が完全に一致しないという特徴がある。これにより、診療データの安全性確保に厄介な問題が生じる。例えば、診療データの利用者側である複数医療機関が適当なグループを組織し、そのグループ内で安全な通信路を静的に構築したとしても、診療データの所有者である患者が、このグループ内の医療機関だけを受診するとは限らない。これにより、上記、医療機関グループの一つを受診した患者が、このグループ内の他の医療機関を受診する限りにおいては、安全に診療データのやりとりが可能なのであるが、このグループ以外の医療機関を受診した場合に、この医療機関との診療データ交換の安全性は確保できなくなる。診療データの所有者である患者は、生涯でいろいろな地域の複数の医療機関を受診するのが一般的であり、患者の受診行動範囲が上記グループ内の医療機関に一致するという想定は受け入れられない。従って、上記実施例のように、患者が受診した医療機関同士で動的に患者ごとの安全なアクセス経路を設定していく仕掛けが必要である。

【００３１】最後に、上記実施例では、２つの病院を対象に説明しているが、３つ以上の医療機関における診療データ共有も同様である。

【００３２】「実施例２」次の実施例では、図５のように患者Ａの在宅から、ネットワーク５０３を介して、アクセス制御設定ファイル２０１を病院５０１と病院５０２に配布する。この実施例では、患者Ａは何らかの別手段で病院５０１のアドレスＨＯＳＰ３と病院５０２のアドレスＨＯＳＰ４を知っているものとする。

【００３３】「アクセス制御設定ファイル生成」（図６）患者Ａ宅において、保健医療カード１０７でアクセス制御設定ファイル２０１を生成する手続きを図６を用いて説明する。

【００３４】（１）患者Ａは、アクセス制御設定ファイル２０１の生成を保健医療カード１０７に指示すると。この時、保健医療カード１０７の鍵生成モジュール３０２において、乱数Ｒ１を生成し、これをカード内のマスタ鍵により暗号化して鍵Ｄｋを生成し、アクセス制御設定ファイル記憶領域６０１の暗号化用鍵の記憶領域６０３に登録する。同様に、保健医療カード１０７の鍵生成モジュール６０２は、乱数Ｒ２を生成し、これをカード内のマスタ鍵により暗号化して鍵Ａｋを生成し、アクセス制御設定ファイル記憶領域６０１の相互認証用鍵の記憶領域６０４に登録する。

【００３５】（２）病院５０１のアドレスＨＯＳＰ３をアクセス制御設定ファイル記憶領域６０１のアクセステーブルの記憶領域６０５に登録する。同様に、病院５０２のアドレスＨＯＳＰ４をアクセステーブルの記憶領域６０５に登録する。

【００３６】（３）アクセス制御設定ファイル記憶領域６０１に記録されたアクセス制御設定ファイル２０１に、保健医療カード１０７の秘密鍵Ｓａで電子署名する。

【００３７】（４）患者Ａの端末５０７に、（３）で電子署名したアクセス制御設定ファイル２０１をダウンロードする。

【００３８】「アクセス制御設定ファイルの配送」アクセス制御設定ファイル２０１を病院５０１、病院５０２に配送する手続きについて説明する。

【００３９】（１）患者Ａの端末５０７から、病院５０１のアドレスＨＯＳＰ３と病院５０２のアドレスＨＯＳＰ４に基づき、電子署名したアクセス制御設定ファイル２０１を各病院に送信する。

【００４０】（２）各病院では、送信されたアクセス制御設定ファイル２０１について、保健医療カード１０７の秘密鍵Ｓａに対応する公開鍵Ｐａで電子署名を検証した後、病院５０１と病院５０２は、アクセス制御設定ファイル２０１を患者Ａの診療データファイルに登録する。

【００４１】ここで、公開鍵Ｐａが確かに患者Ａのものであることは、信頼できる第３者機関が公開鍵証明書を発行していることにより保証されているものとする。

【００４２】以上により、病院５０１と病院５０２において、患者Ａのアクセス制御設定ファイルが得られたので、以降、診療データの共有は、実施例１と同じである。また、この例では、二つの病院を例に説明したが、三つ以上の医療機関においても同様である。

【００４３】

【発明の効果】各患者ごとの、アクセス制御設定ファイル２０１を各医療機関で共有し、それを当該患者の診療情報データの一属性として管理することで、まず、アクセス制御設定ファイル２０１の医療機関のアドレステーブル２０５により複数医療機関にまたがる当該患者の診療データ同士がネットワーク上でリンクされる。しかも、アクセス制御設定ファイル２０１で管理する暗号化用鍵と相互認証用鍵により、当該患者の診療データ同士がネットワーク上でのリンクは、データの完全性と機密性が確保できる。また、相互認証用鍵を利用した相互認証処理により、患者の主治医または受診した病院以外の、医療従事者からのアクセスが禁止されることにより、患者のプライバシーが確保できる。以上、患者の診療データ同士がネットワーク上で安全にリンクされるので、患者の主治医または受診した病院からは、常時、当該患者のデータを安全に共有することが可能になる。

【図面の簡単な説明】

【図１】本発明の実施例のシステム構成図

【図２】本発明の実施例において使用するファイルの構成図

【図３】本発明の実施例における保健医療カード内での処理を表わす図

【図４】本発明の実施例における診療データ共有のためのプロトコルを示す図

【図5】本発明の実施例のシステム構成図
【図6】本発明の実施例における保健医療カード内での処理を表わす図
【符号の説明】
101…病院、102…病院、103…ネットワーク、104…ファイルサーバ、105…ファイルサーバ、106…診療データファイル、107…保健医療カード、201…アクセス制御設定ファイル、202…患者ID、203…暗号化用鍵、204…相互認証用鍵、205…アドレステーブル、206…診療データファイル、207…患者ID、208…アクセス制御設定情報、209…各診療データ、301…アクセス制御設定ファイル記憶領域、302…鍵生成モジュール、501…病院、502…病院、503…ネットワーク、504ファイルサーバ、505ファイルサーバ、506診療データファイル、507…患者宅端末、601…アクセス制御設定ファイル記憶領域、602…鍵生成モジュール、

【図1】

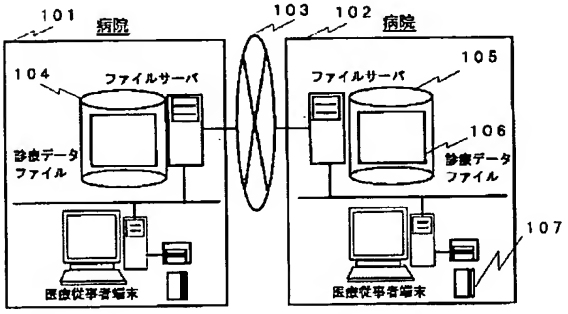


図1

【図2】

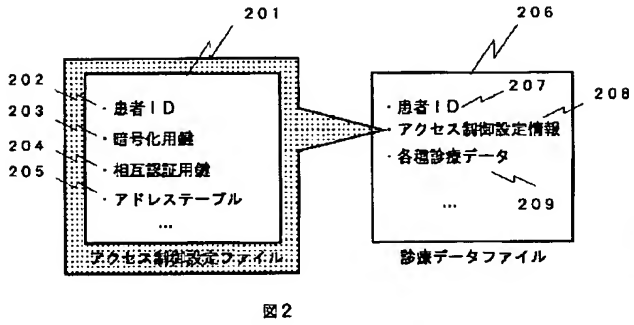


図2

【図3】

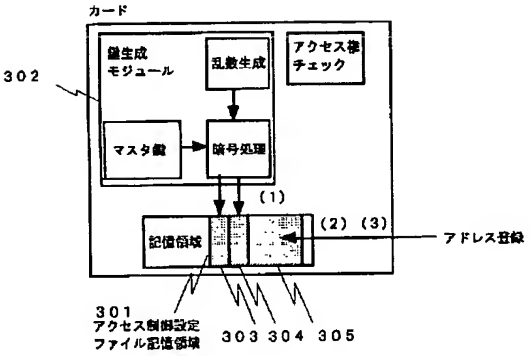


図3

【図5】

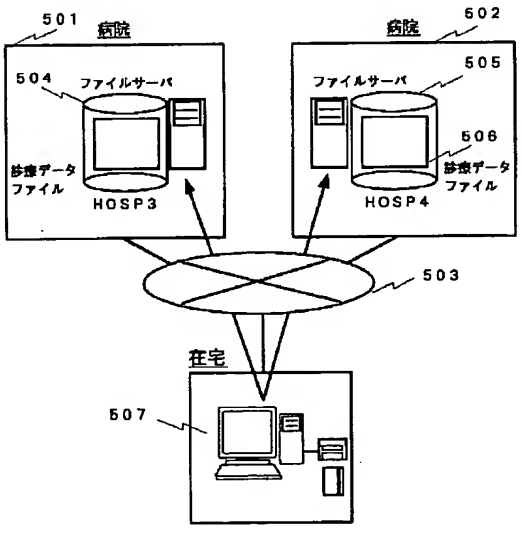
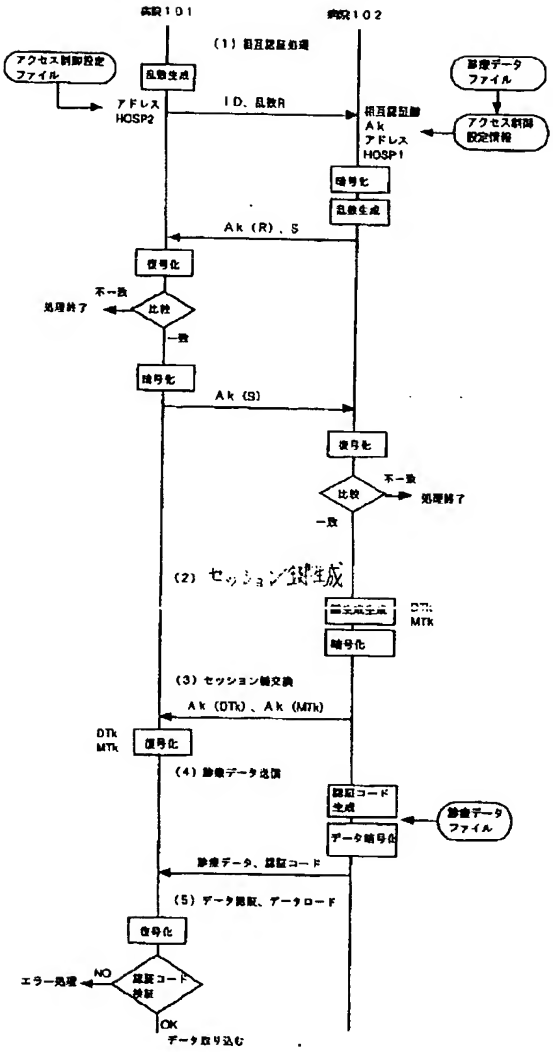


図5

【図4】

図 4


病院101
病院102
(1) 相互認証処理
アクセス制御設定ファイル
乱数生成
診療データファイル
アドレス HOSP2
ID、乱数R
相互認証部 Ak アドレス HOSP1
アクセス制御設定情報
暗号化
乱数生成
Ak (R)、S
復号化
比較
不一致
処理終了
一致
暗号化
Ak (S)
復号化
比較
不一致
処理終了
一致
(2) セッション鍵生成
DTk MTk
暗号化
(3) セッション鍵交換
Ak (DTk)、Ak (MTk)
DTk MTk
復号化
(4) 診療データ送信
認証コード生成
診療データファイル
データ暗号化
診療データ、認証コード
(5) データ認証、データロード
復号化
エラー処理
NO
認証コード検証
OK
データ取り込む

【図6】

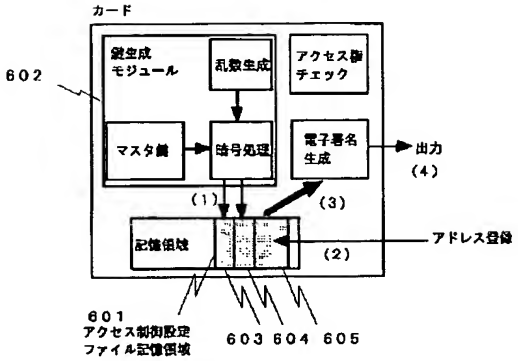

カード
602
鍵生成モジュール
乱数生成
アクセス制御チェック
マスタ鍵
暗号処理
電子署名生成
出力
(4)
(1)
(3)
記憶領域
(2)
アドレス登録
601
アクセス制御設定ファイル記憶領域
603 604 605

図6